AO 106 (Rev. 04/10) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the

District of New Mexico

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

2824 San Miguel Court,
Las Cruces, NM 88007

Case No. 15-MR405

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

2824 San Miguel Court, Las Cruces, NM 88007

located in the _____ District of New Mexico, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 United States Code 2252	

The application is based on these facts:

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Lisa Keyes, Special Agent
Applicant's signature

Lisa Keyes, Special Agent
Printed name and title

Sworn to before me and signed in my presence.

Date: 30 June 2015

Judge's signature

City and state: Las Cruces NM

GREGORY B. WORMUTH
U.S. MAGISTRATE JUDGE
Printed name and title

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEW MEXICO

IN THE MATTER OF THE SEARCH OF:
2824 San Miguel Court, Las Cruces, New Mexico, 88007

Case No. 15-MR-405

AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A WARRANT TO SEARCH AND SEIZE

AFFIDAVIT

I, Lisa Keyes, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the premises known as **2824 San Miguel Court, Las Cruces, New Mexico, 88007**, hereinafter the "Premises," further described in Attachment A, for the things described in Attachment B.

2. I am Special Agent with Homeland Security Investigations (HSI) and have been so employed since January of 2010. I am classified, trained and employed as a federal law enforcement officer with statutory arrest authority charged with conducting criminal investigations of alleged violations of federal criminal statutes, including Title 18 of the United States Code. I am currently assigned as a criminal investigator for the Office of the Resident Agent in Charge, Las Cruces, New Mexico. Prior to my current position, I was a Police Officer and Police Sergeant with the Atlanta Police Department for over twelve and a half years. I received a Bachelor Degree in Criminal Justice and have completed thirty six (36) hours of graduate education in Public Administration. During the course of this investigation I have

consulted with other HSI Agents and other law enforcement detectives and officers who have extensive experience investigating Internet crimes against children including: child trafficking, the possession, receipt, distribution, and production of abusive images of children, and enticing children to engage in illegal sexual acts. I attended a Basic Peer to Peer Investigations refresher Training in February 2012, the National Law Enforcement Training on Child Exploitation Conference in April 2012, an Undercover Chat Investigations Training in October 2012, and a Child Exploitation refresher course in February 2014. I have experience investigating internet crimes against children including: the possession, receipt, distribution, and production of child pornography, child exploitation; and the enticing children to engage in illegal sexual acts. Over the course of my career as a HSI Agent, I have lead or participated in over a hundred separate federal and state investigations of child pornography and exploitation cases which resulted in further investigations, indictments and eventual convictions.

FACTS AND CIRCUMSTANCES

3. The statements in this affidavit are based in part on information provided by a Special Agent with the New Mexico Attorney General's Office Internet Crimes Against Children Task Force and on my experience and background as a Special Agent with HSI. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. As will be shown below, there is probable cause to believe that an individual located at 2824 San Miguel Court, Las Cruces, New Mexico 88007 distributed and possessed child pornography, in violation of 18 U.S.C. §§ 2252(a)(2) and 2252(4)(B). I am submitting this affidavit in support of a search warrant authorizing a search of 2824 San Miguel Court, Las Cruces, New Mexico, 88007, (the "Premises"), which is more particularly described in Attachment A. I am requesting authority to

search the entire Premises, vehicles on the premises, including the residential dwelling and any computer and computer/digital media located therein where the items specified in Attachment B may be found, and to seize all items listed in Attachment B as instrumentalities, fruits, and evidence of crime.

DEFINITIONS

4. The following definitions apply to this Affidavit and Attachment B to this Affidavit:

5. "Child Erotica" means materials or items that are sexually arousing to persons having a sexual interest in minors, but that are not, in and of themselves, obscene or illegal. In contrast to "child pornography," this material does not necessarily depict minors in sexually explicit poses or positions. Some of the more common types of child erotica include photographs that are not sexually explicit, drawings, sketches, fantasy writing, and diaries. *See Kenneth V. Lanning, Child Molesters: A Behavioral Analysis (2001) at 65*. Federal courts have recognized the evidentiary value of child erotica and its admissibility in child pornography cases. *See United States v. Cross, 928 F.2d 1030 (11th Cir. 1991)* (testimony about persons deriving sexual satisfaction from and collecting non-sexual photographs of children admissible to show intent and explain actions of defendant); *United States v. Vosburgh*, 602 F.3d 512, 538 (3d Cir. 2010)(probative value of child erotica probative was "not insignificant" as to Defendant's motive as well as to disproving unknowing possession or accident) ; *United States v. Caldwell, No. 97-5618, 1999 WL 238655 (E.D. Ky. Apr. 13, 1999)*(unpublished) (child erotica admissible under Federal Rule of Evidence 404(b) to show knowledge or intent).

6. "Child Pornography" includes the definition in 18 U.S.C. § 2256(8) (any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved

the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct), as well as any visual depiction, the production of which involves the use of a minor engaged in sexually explicit conduct (see 18 U.S.C. §§ 2252 and 2256(2)).

7. "Visual depictions" include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image. See 18 U.S.C. § 2256(5).

8. "Sexually explicit conduct" means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any persons. *See* 18 U.S.C. § 2256(2).

9. "Computer" as used herein, is defined pursuant to 18 U.S.C. § 1030(e)(1), as "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device."

10. "Computer hardware" as used herein, consists of all equipment which can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including, but not limited to, keyboards,

printers, video display monitors, and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).

11. "Computer software" as used herein, is digital information which can be interpreted by a computer and any of its related components to direct the way they work. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

12. "Computer-related documentation" as used herein, consists of written, recorded, printed, or electronically stored material which explains or illustrates how to configure or use computer hardware, computer software, or other related items.

13. "Computer passwords and data security devices" as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates a sort of digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the progress to restore it.

14. "Cellphones" as used herein, are portable telephones. Cellphones usually contains a "call log," which records the telephone number, date, and time of calls and text messages made to and from the phone. In addition to enabling voice communications, cellphones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic

"address books;" sending, receiving, and storing text messages, e-mails, and other digital data; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet.

15. "Smartphones" are cellphones with advanced computing capability. Smartphones typically include the features of a wireless telephone, portable media player, PDA, digital camera, GPS navigation unit, and touch screen computer with web browsing and Wi-Fi capabilities. Smartphones, typically contain programs called apps, which, like programs on a personal computer, perform different functions and save data associated with those functions. Apps can, for example, permit accessing the Web, sending and receiving e-mail, and participating in Internet social networks.

16. "Internet Protocol address" or "IP address" refers to a unique number used by a computer to access the Internet. IP addresses can be dynamic, meaning that the Internet Service Provider (ISP) assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be static, meaning an ISP assigns a user's computer the same IP address each time the computer accesses the Internet.

17. The terms "records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard

disks, CD-ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, smart phones, memory calculators, electronic dialers, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

BACKGROUND ON COMPUTERS AND CHILD PORNOGRAPHY

18. Computers and computer technology have revolutionized the way in which individuals interested in child pornography interact with each other. Child pornography formerly was produced using cameras and film (either still photography or movies). The photographs required darkroom facilities and a significant amount of skill in order to develop and reproduce the images. There were definable costs involved with the production of pornographic images. To distribute these on any scale required significant resources. The photographs themselves were somewhat bulky and required secure storage to prevent their exposure to the public. The distribution of these wares was accomplished through a combination of personal contacts, mailings and telephone calls.

19. The development of computers has changed this. Computers basically serve four functions in connection with child pornography: production, communication, distribution, and storage.

20. Child pornographers can now transfer photographs from a camera onto a computer-readable format with a device known as a scanner. With the advent of digital cameras, the images can now be transferred directly onto a computer. A device known as a modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Electronic contact can be made to literally millions of computers around the world.

21. The computer's ability to store images in digital form makes the computer itself

an ideal repository for child pornography. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers has grown tremendously within the last several years. These drives can store thousands of images at very high resolution.

22. The Internet and its World Wide Web afford collectors of child pornography several different venues for obtaining, viewing and trading child pornography in a relatively secure and anonymous fashion.

23. Based on my training and experience, individuals who possess, receive, distribute and produce child pornography have a sexual attraction to children. They receive sexual gratification and satisfaction from sexual fantasies fueled by depictions of children that are sexual in nature.

24. Based on my training and experience, the majority of individuals who possess and produce child pornography collect sexually explicit materials, which may consist of photographs, magazines, motion pictures, video tapes, books, slides, computer graphics or digital or other images for their own sexual gratification. The majority of these individuals also collect child erotica, which may consist of images or text that do not rise to the level of child pornography but which nonetheless fuel their deviant sexual fantasies involving children.

25. Based on my training and experience, individuals who possess and produce child pornography often seek out like-minded individuals, either in person or on the Internet, to share information and trade depictions of child pornography and child erotica as a means of gaining status, trust, acceptance and support. This contact also helps these individuals to rationalize and validate their deviant sexual interest and associated behavior. The different internet-based vehicles used by such individuals to communicate with each other include, but are not limited to,

P2P (Peer to Peer), e-mail, e-mail groups, bulletin boards, IRC, newsgroups, instant messaging, and other similar vehicles, and these vehicles can be accessed through the use of an internet capable device. For many of the same reasons, individuals who possess and produce child pornography often seek to communicate, through the internet or in person, with children.

26. Based on my training and experience, individuals who collect child pornography often collect, read, copy or maintain names, addresses (including e-mail addresses), phone numbers, or lists of persons who have advertised or otherwise made known in publications and on the Internet that they have similar sexual interests. These contacts are maintained as a means of personal referral, exchange or commercial profit. These names may be maintained in the original medium from which they were derived, in telephone books or notebooks, on computer storage devices, or merely on scraps of paper.

27. Based on my training and experience, individuals who collect child pornography often collect "hard copies" of child pornographic material, that is, pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location.

28. Based on my training and experience, individuals who distribute and collect child pornography rarely, if ever, dispose of their sexually explicit materials and may go to great lengths to conceal and protect from discovery, theft, and damage their collections of illicit materials.

29. I know from training and experience that search warrants of residences involved in computer or digitally related criminal activity usually produce items that tend to establish

ownership or use of digital devices and ownership or use of any internet service accounts accessed to include credit card bills, telephone bills, correspondence and other identification documents.

30. I know from training and experience that search warrants of residences usually reveal items that tend to show dominion and control of the property searched, including utility bills, telephone bills, correspondence, rental agreements and other identification documents.

31. Collectors and distributors of child pornography also use online resources to retrieve and store child pornography, including services offered by Internet Portals such as America Online (AOL), Yahoo! and Hotmail, among others. The online services allow a user to set up an account with a remote computing service that provides e-mail services as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with access to the Internet. Evidence of such online storage of child pornography is often found on the user's computer. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer in most cases.

32. As is the case with most digital technology, computer communications can be saved or stored on hardware and computer storage media used for these purposes. Storing this information can be intentional, i.e., by saving an e-mail as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files. However, digital information can also be retained unintentionally, e.g., traces of the path of an electronic communication may be automatically stored in many places (e.g., temporary files or ISP client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser

used. Such information is often maintained for very long periods of time until overwritten by other data. Additionally, virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created. A forensic examiner often can recover evidence suggesting whether a computer contains peer-to- peer software, when the computer was sharing files, and some of the files that were uploaded or downloaded. Such information is often maintained for very long periods of time until overwritten by other data.

33. Digitally related devices and/or media can be extremely small in size and transportable, these items can be located anywhere on the property to include vehicles outbuildings, and concealed on a person. This is especially true as many computers, smart phones and other devices are capable of connecting to the internet wirelessly, and they are not anchored to one particular location inside a home but can be used anywhere within the vicinity of the wireless network.

34. Based on my own training and experience I know that P2P "peer-to-peer" networks are frequently used in the trading of child pornography.

35. Computer users can choose to install publicly available software that facilitates the trading of images. The software, when installed, allows the user to search for pictures, movies

and other digital files by entering text as search terms. That text search is sent to an ultra-peer. An ultra-peer is an index server that handles requests and examines submitted file lists from peers that it knows about for files matching the text search request. A file list is then sent back to the requesting user who can choose to download files from peers who possess at least a portion of the file.

36. Search results presented to the user allow the user to select a file and then receive that file from other users around the world. These users can receive the selected file from numerous sources at once. The software can balance the network load and recover from network failures by accepting pieces of the file from different users and then reassembling the file on the local computer.

37. P2P networks can only succeed in reassembling the file from different parts if the parts all come from the same original file. I know that multiple persons sharing one file can deliver different pieces of that file to the local software and the local software can insure that a complete and exact copy can be made from the parts.

38. P2P computer software has different methods to insure that two files are exactly the same. I know from training that the method used by the P2P Operation described herein involves a compressed digital representation method called Secure Hash Algorithm Version 1 or SHA1. I know that the Secure Hash Algorithm (SHA) was developed by the National Institute of Standards and Technology (NIST), along with the National Security Agency (NSA), for use with the Digital Signature Standard (DSS) as specified within the Secure Hash Standard (SHS). The United States of America has adopted the SHA1 hash algorithm described herein as a Federal Information Processing Standard.

39. Digital files can be processed by this SHA1 standard resulting in a digital

signature. By comparing these signatures I can conclude that two files are or are not identical with a precision that greatly exceeds 99.9999 percent certainty. As such, the use of SHA1 compressed digital representations for the matching of movies and images have proven to be extremely reliable. I know through the from my training and experience, as well as speaking with certified computer forensic analysts that there has never been a documented occurrence of two different files being found on the Internet having different contents while sharing the same SHA1 value.

40. The P2P network investigated in this operation uses the SHA1 digital signature to verify the unique identity of individual files. I know that users attempting to trade files on a P2P file-sharing network can place files from their local computer in a shared file directory. If that user then starts the P2P software that local computer calculates the SHA1 signature for each shared file and provides that information to other users wishing to trade files.

41. Entering search terms in the P2P software results in a list of SHA1 digital signatures that an Agent can choose for download. By using this type of search an Agent compares the offered SHA1 signatures with SHA1 signatures known to belong to movies or images of child pornography. An Agent confirms these SHA1 values as belonging to child pornography by examining the files from previous investigations with the matching SHA1 value. By watching these movies or viewing these images the agent is able to determine the exact file referenced by the given SHA1 value. Once a matching set of digital signatures is identified, an Agent can submit a download request for the file.

42. This method has proven to be extremely reliable, working just like software used by end users around the world in locating and downloading precise files. Once the download of child pornography is initiated an Agent receives a list of download candidates that are

participating in the possession, receipt and/or distribution of child pornography. This feature allows an Agent to conduct undercover operations that involve images of child sexual abuse being traded on peer-to-peer networks.

43. Internet computers identify each other by an Internet Protocol or IP address. I know that these IP addresses can assist law enforcement in finding a particular computer on the Internet. These IP addresses lead the law enforcement officer to a particular Internet service provider or company (ISP). Given the date and time the IP address was used, an ISP can typically identify the account holder by name and physical address.

44. Searching on a peer-to-peer network as described above results in a list of IP addresses identifying locations where a computer has P2P software installed and individual files have been reported as available for download with a specific digital signature (SHA1).

45. These computers are referred to as a download candidate. A download candidate is a computer that was reported by an ultra-peer as a source for the file listed by SHA1 value. In almost every known case the download candidate serves those files to P2P users across the Internet.

46. Computers from throughout the world can download files from download candidates without regard to geographic location. I know that the files located on P2P download candidates are quickly available throughout the world due to the distributed sharing model of P2P networks.

47. P2P software may display the Globally Unique Identifier (GUID) identification number of computers offering to share files on the network. A Globally Unique Identifier or GUID is a pseudo-random number used in software applications. This GUID number is produced when some P2P software applications are installed on a computer. While each generated GUID

is not guaranteed to be unique, the total number of unique keys is so large that the probability of the same number being generated twice is very small. When comparing these GUIDs, I can quickly determine with a high degree of certainty that two different IP addresses that are associated with the same GUID are associated with the same computer.

48. I know that cooperating police agencies pool their information to assist in identifying criminal conduct and build probable cause to further criminal investigations. With this pooled information police get a better understanding of the global information available about a suspect that resides in their area of jurisdiction. This information is valuable when trying to regionalize a suspect to a certain jurisdiction, given the global scope of the Internet. Investigators from around the world gather and log information, which can be used by an investigator to build probable cause on one specific case.

49. I know that by examining a list of IP addresses an Agent can locate computers that are reported to be in New Mexico. By comparison of the SHA1 digital signatures I can conclude that a computer, originating from an IP address known to be in New Mexico, has P2P software installed on it and contains images of child pornography. With this information a request can be made to the Internet service provider to identify the specific physical address related to the use of P2P software in the exchange of child pornography.

50. I am aware that numerous search warrants have been executed in the State of New Mexico using the above method of investigation. This method has proven to be extremely reliable in determining the location of computers that were involved in the P2P-facilitated trading of child pornography. I have been involved in search warrants, assisting other investigators with their warrants, that the above listed method of investigation, almost every case was verified through the following means: Evidence of child pornography was found on the computer. If no

images of child pornography were found on the computer, interviews of persons using those computers verified that child pornography had been present at one time but had been deleted, moved from the computer and stored on other media, or the computer with the child pornography had been removed from the premises.

SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS

51. Searches and seizures of evidence from computers commonly require agents to download or copy information from the computers and their components, or seize most or all computer items (computer hardware, computer software, and computer related documentation) to be processed later by a qualified computer expert in a laboratory or other controlled environment. This is almost always true because of the following:

52. Computer storage devices (like hard disks, diskettes, tapes, laser disks, magneto opticals, and others) can store the equivalent of thousands of pages of information. Especially when the user wants to conceal criminal evidence, he or she often stores it in random order with deceptive file names. This requires searching authorities to examine all the stored data to determine whether it is included in the warrant. This sorting process can take days or weeks, depending on the volume of data stored, and it would be generally impossible to fully accomplish this kind of data search on site.

a. Searching computer systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert should analyze the system and its data. The search of a computer system is an exacting scientific procedure which is designed to protect the integrity of the evidence and to recover even hidden, erased, compressed,

password-protected, or encrypted files. Since computer evidence is extremely vulnerable to tampering or destruction (which may be caused by malicious code or normal activities of an operating system), the controlled environment of a laboratory is essential to its complete and accurate analysis. To the extent feasible, the Agents executing the search will conduct a limited on-scene forensics analysis of the recovered evidence. However, a full and complete analysis will not be attempted on scene.

b. In order to fully retrieve data from a computer system, the analyst needs all magnetic storage devices as well as the central processing unit (CPU). In cases involving child pornography where the evidence consists partly of graphics files, the monitor(s) may be essential for a thorough and efficient search because of software and hardware configuration issues. In addition, the analyst needs all the system software (operating systems or interfaces, and hardware drivers) and any applications software which may have been used to create the data (whether stored on hard drives or on external media).

53. In addition, there is probable cause to believe that the computer and its storage devices, the monitor, keyboard, and modem are all instrumentalities of the crimes, within the meaning of 18 U.S.C. §§ 2251 through 2256, and should all be seized as such.

BACKGROUND OF THE INVESTIGATION

54. On March 26, 2015, Special Agent (SA) Jay Ratliff of the New Mexico Attorney General's Office was conducting investigations into the sharing of "Child Pornography" files on the Gnutella P2P file sharing network. SA Ratliff reported that he identified the computer with the IP address 69.247.67.60 as a potential download candidate for at least 70 file(s) of investigative interest. SA Ratliff reported that the Gnutella client with IP address 69.247.67.60 reported itself as: Shareaza 2.7.8.0. and nickname reported as: Omega. SA Ratliff reported that

on March 26, 2015, he conducted a query on the IP address 69.247.67.60 through the American Registry for Internet Numbers (ARIN). According to SA Ratliff the IP address 69.247.67.60, was registered to Comcast Cable Communications, Inc.

55. On March 26, 2015, between 0028 hours and 0034 hours UTC, SA Jay Ratliff successfully completed the single-source download of the following 3 file(s) that the computer at IP address 69.247.67.60 was making available:

[PTHC] 10yo Missy (SO hot!).JPG	Z5WLR....
Pthc_kely & camilacamila037.jpg	JMLUP....
PTHC Childlover P002.jpg	SVOZA....

These files were downloaded only from the computer at IP Address 69.247.67.60.

56. On March 26, 2015, between 1904 hours and 1916 hours UTC, SA Ratliff successfully completed the single-source download of the following 3 file(s) that the computer at IP address 69.247.67.60 was making available:

((PTHC)) 3 VAN GIRLS (13).jpg	WV6MB....
[pthc] Mexican Child Brothel – LC-464329.jpg	5NPIA....
[pthc] Mexican Child Brothel – LC-464343.jpg	TIP34....

These file were downloaded only from the computer at IP Address 69.247.67.60.

57. I have reviewed the above listed downloaded files. Below is a description of each file:

- [PTHC] 10yo Missy (SO hot!).JPG (SHA1: Z5WLR....) This photograph depicts a pubescent age female lying nude on her back upon a bed. The female's face can be seen and is facing the camera. The female has her legs spread apart exposing her vagina and breast. I believe this female to be between 10 and 11 years of age due to her body size, little breast development and nonexistent pubic hair.

- Pthc_kely & camilacamila037.jpg (SHA1: JMLUP....) This photograph depicts two nude, dark haired pre-pubescent females sitting on a white sheet. One of the females is holding an adult male penis with her left hand while the other female inserts her right hand fingers into the other female's vagina. I believe the females to be between

10 to 12 years of age due to lack of breast development, small body size comparison and nonexistent pubic hair.

- PTHC Childlover P002.jpg (SHA1: SVOZA....) This photograph depicts a prepubescent female lying on a multi-colored bedspread. The female has her legs spread apart exposing her vagina. An adult male is standing over the female with the tip of his penis penetrating her vagina. I believe this female's age is between 8 and 11 years of age due to small body size comparison and non-existent pubic hair.

- ((PTHC)) 3 VAN GIRLS (13).jpg (SHA1: WV6MB....) This photograph depicts a young female lying on a tan, yellow and grey blanket. The female is completely nude with her head turned away from the camera with her blonde hair covering her face. The female's right leg is slightly bent exposing her vagina to the camera. I believe this female is between the ages 8 and 11 due to no breast development and no pubic hair development.

- [pthc] Mexican Child Brothel – LC-464329.jpg (SHA1: 5NPIA....) This photograph depicts a close-up view of a young female's vagina. I believe the female is between the ages of 10 and 13 due to the lack of pubic hair development.

- [pthc] Mexican Child Brothel – LC-464343.jpg (SHA1: TIP34....) This photograph depicts a prepubescent female sitting in a chair nude from the waist down with the focal point of the photograph being her vagina. I believe the female is between 8 and 11 due to small body size and slight pubic development.

58. On April 15, 2015, The New Mexico Attorney General's Office in Albuquerque, NM, received information from Comcast Cable Communications, Inc, indicating that on March 26, 2015, at 12:29 AM UTC, IP Address 69.247.67.60 was registered to David Garcia at 2824 San Miguel Court, Las Cruces, NM 88007. SA Ratliff was able to download the above described child pornography on March 26, 2015, between the hours of 0028 hours and 1916 hours UTC.

59. I have obtained records from the Department of Labor and learned from those records that a David Garcia, who is listed at 2824 San Miguel Court, Las Cruces, NM, 88007, has been employed/reporting wages earned by the Las Cruces Public School System since first quarter reporting of 2014. First quarter reporting covers the first three months of the year,

January, February, and March of 2014.

60. Intelligence Research Specialist Robert Rede obtained, from the New Mexico Department of Motor Vehicles, a photograph from the New Mexico drivers license of an individual named David Garcia. Information obtained from the New Mexico Department of Motor Vehicles shows that David Garcia, who is listed as residing at 2824 San Miguel Court, Las Cruces, NM, 88007, is the registered owner of a blue Pontiac G-6 automobile for which a New Mexico state license plate reading 841-PZC has been issued. According to the information provided by the New Mexico Department of Motor Vehicles, David Garcia is 5'09 inches tall and weighs 250 lbs with brown eye color.

61. On the morning of June 25, 2015, I conducted surveillance on 2824 San Miguel Court, Las Cruces, NM, 88007. While conducting surveillance I observed that a blue Pontiac G-6 automobile with a New Mexico state license plate reading 841-PZC was parked on the property, at 2824 San Miguel Court, Las Cruces, NM, 88007, in front of the home.

62. In the afternoon of June 23, 2015, I conducted surveillance at Mesilla Park Elementary School which is located at 955 W. Union Ave, Las Cruces, New Mexico, 88005. While conducting surveillance, I observed an individual, who's face matched the driver's license photograph of David Garcia, provided by the New Mexico Department of Motor Vehicles, standing in front of Mesilla Park Elementary School. The same individual proceeded to walk around the outside of the school building before walking around the rear of the building out of sight. This individual was approximately 5'09 inches tall and weighed approximately 250 lbs. This individual was wearing a blue work shirt and jeans and appeared to have a set of keys for the school. The individual appeared to utilize a key to release the handle on the exterior door of the school. During the same time period I observed that a blue Pontiac G-6 automobile with a

New Mexico State license plate reading 841-PZC was parked in the Mesilla Park Elementary School parking lot.

63. I know that Homeland Security Investigations has executed numerous search warrants using the techniques described in this investigation. In prior cases the suspect confessed and/or the computers were seized and found to contain traces of evidence confirming the operation.

CONCLUSION

64. Based on the aforementioned factual information, I respectfully submit that there is probable cause to believe that an individual who resides at the residence located at 2824 San Miguel Court, Las Cruces, New Mexico 88007 is involved in the possession and distribution of child pornography through the use of Internet Peer to Peer Networks. I respectfully submit that there is probable cause to believe that an individual residing in the residence described above has violated 18 U.S.C. §§ 2252(a)(2) and 2252(4)(B).

65. Further, there is probable cause to believe that evidence, fruits and instrumentalities of this crime, which are listed specifically in Attachment B, which is incorporated herein by reference, are presently located on the premises at 2824 San Miguel Court, Las Cruces, New Mexico 88007. Rule 41 of the Federal Rules of Criminal Procedure authorizes the government to seize and retain evidence and instrumentalities of a crime for a reasonable time, and to examine, analyze, and test them. If computers/digital media are found at the residence, forensic investigative tools and techniques will be used to examine the computers/digital media.

66. Based upon my knowledge, training and experience, and consultations with Forensic experts, I know that searching and seizing information from computers often requires

agents to seize most or all electronic storage devices (along with related peripherals) to be searched later by a qualified computer expert in a laboratory or other controlled environment. This is true because of the volume of evidence.

67. With respect to the volume of evidence, computer storage devices (like hard disks, diskettes, tapes, DVDs, etc.) can store the equivalent of millions of pages of information. Additionally, a suspect may try to conceal criminal evidence or he or she might store it in random order with deceptive file names. This may require searching authorities to examine all the stored data to determine which particular files are evidence and instrumentalities of crime. This sorting process can take weeks or months, depending on the volume of data stored, and it would be impractical to attempt this kind of data search on site.

68. I, therefore, respectfully request that the attached warrant be issued authorizing the search and seizure of the items listed in Attachment B.

Lisa Keyes
Special Agent
Homeland Security Investigations

Subscribed and sworn before me this 30th day of June, 2015.

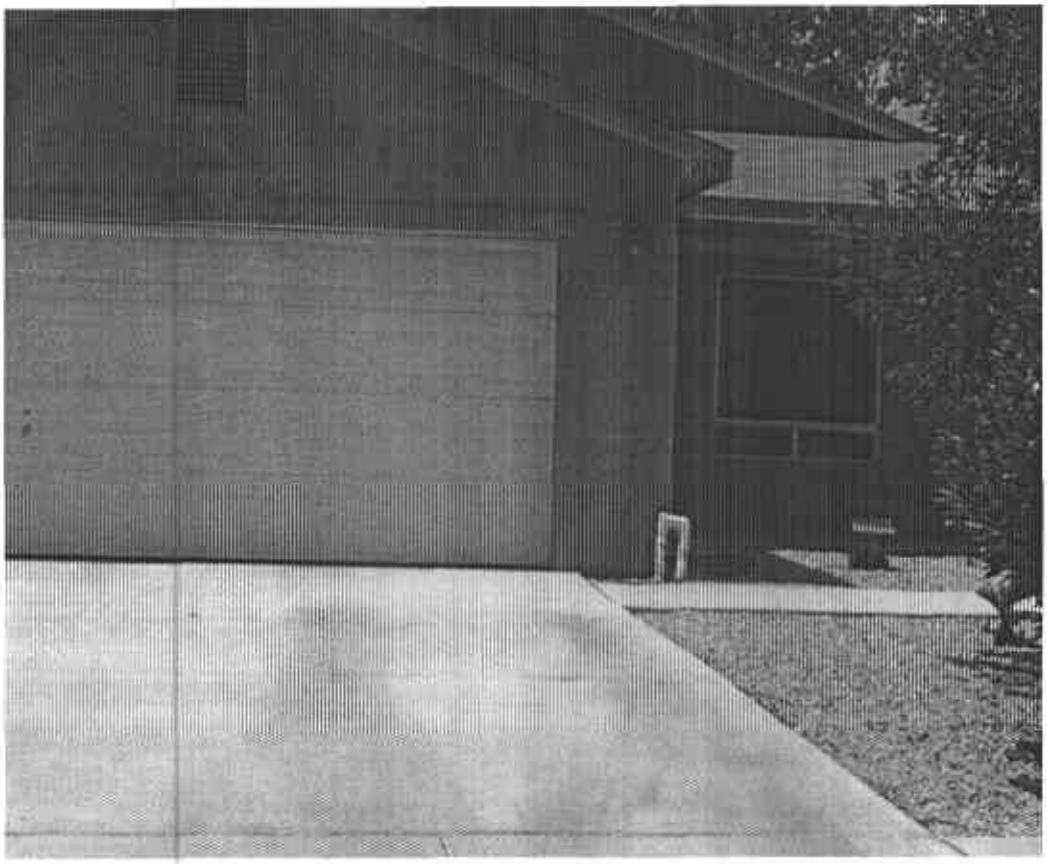
United States Magistrate Judge

ATTACHMENT A

DESCRIPTION OF THE PREMISES TO BE SEARCHED

The residence to be searched, located at 2824 San Miguel Court, Las Cruces, New Mexico, 88007, can be further described as a single story ranch style. The construction is tan color stucco exterior with a white two car garage door facing the street. Facing the residence, there is a large window and the front door is to the right of the window. The front door is white in color with a clear glass screen door outside of it. The numbers 2824 are in black and affixed to the molding below the garage roof facing the street. Directly in front of the 2824 San Miguel Court address are the numbers 2824 painted on the curb in black with a white square background.

(Photo of above described property)



ATTACHMENT B

IDENTIFICATION OF ITEMS TO BE SEARCHED FOR:

The particular items to be seized include all fruits, evidence, and instrumentalities of violations of 18 USC §§ 2252(a)(2) (Distribution of Child Pornography) and 2252(4)(B)(Possession of Child Pornography) including but not limited to the following:

A. All electronic data processing and storage devices, computers and computer systems including central processing units; internal and peripheral storage devices such as fixed disks, external hard disks, optical storage devices, cellular telephones, smart phones, PDAs, IPods, IPads, Tablets, gaming systems or other memory storage devices; peripheral input/output devices such as keyboards, printers, video display monitors, optical readers and related communication devices such as modems; together with system documentation, operating logs and documentation, software and instruction manuals, handwritten notes, logs, user names and lists.

B. Any photographs, digital images, videos, computerized graphic files, printed material, computer images or files made by electronic or mechanical means which are located on the premises which show a person who is or depicted as being under the age of eighteen years engaged in or depicted as being engaged in sexual conduct or the lewd exhibition of the genitals.

C. Any and all notes, documents, records, or correspondence, in any format and medium (including, but not limited to, e-mail messages, text messages, chat logs and other digital data files) pertaining to the possession, receipt, distribution, or production of child pornography as defined in 18 U.S.C. § 2256(8) or to the possession, receipt, distribution, or production of visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2)(A)

D. Any and all records, documents, invoices and materials, which concern any accounts with an Internet Service Provider.

E. Passwords, encryption keys, and other access devices that may be necessary to access information stored on the Device or elsewhere. Any and all passwords and other data security devices designed to restrict access to, hide, or destroy software, documentation, or data. Data security devices may consist of software or other programming code. Any and all data which would reveal the presence of malware, viruses or malicious codes located on the computer storage media.

F. Records evidencing the use of the Internet Protocol addresses including records of and records of Internet activity, including firewall logs, caches, browser history and cookies,

"bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

G. Any and all records, documents, invoices and materials, in any format or medium that concern online storage or other remote computer storage, including, but not limited to, software used to access such online storage or remote computer storage, user logs or archived data that show connection to such online storage or remote computer storage, and user logins and passwords for such online storage or remote computer storage.

H. All books, magazines, documents, advertisements portraying children under the age of eighteen engaged in sexual conduct, posed in sexually explicit positions or that contains unclothed or partially unclothed children under the age of eighteen.

I. All materials or items which are sexually arousing to individuals who are interested in minors, but which are not in and of themselves obscene or which do not necessarily depict minors involved in sexually explicit conduct. Such material is commonly known as "child erotica" and includes written materials, written communications and emails, personal journals dealing with child development, sex education, child pornography, sexual abuse of children, incest, child prostitution, investigative techniques of child exploitation, sexual disorders, pedophilia, diaries, and fantasy writings.

J. Lists, papers, and documents identifying names, addresses, email addresses and telephone numbers of minors.

K. Photographs, digital images, and depictions of minors with whom the suspect may have had contact and that may lead to the identity and age of any minor children depicted in any visual media seized pursuant to this search warrant.

L. All diaries, logs, notations, telephone/address books, telephone answering machine tapes, correspondence, voice mail, e-mail, text messages, chat conversations, images and/or any other documentation tending to show any communication or correspondence with minors.

M. All electronic equipment, projectors, televisions, VCR's and/or any other device, that will be needed to watch, playback or duplicate an item that was seized.

N. All persons, lockboxes, locked containers, vehicles, and outlying structures located on the property or curtilage, where diaries, notes, pictures or other evidence of crimes against children may be stored for safekeeping against seizure.

O. All Routers, modems, and network equipment used to connect computers or other devices to the Internet.

GBW

27

P. During the course of the search, photographs of the searched premises may also be taken to record the condition thereof and/or the location of items therein.

Q. All documents tending to show occupancy and/or ownership of the home, including personal identification, bills, receipts, canceled mail, utility bills, rent receipts and bank statements.

R. All documents including e-mail to or from the occupants of the residence or documents relating to account(s) with any online services, bills, receipts, canceled checks, bank statements, applications and advertisements.